

FILED	LODGED
RECEIVED	COPY
MAY - 3 2019	
19-8811MB	
CLERK U.S. DISTRICT COURT	
DISTRICT OF ARIZONA	
DEPUTY	

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, Daniel Sutcliffe, a Special Agent employed by the Homeland Security Investigations being duly sworn under oath, do hereby depose and state:

**PRELIMINARY BACKGROUND INFORMATION**

1. I, Daniel Sutcliffe am employed as a Special Agent in the Department of Homeland Security (DHS), Homeland Security Investigations (HSI). I have been employed as a special agent with HSI since April 2018. I graduated from the Federal Law Enforcement Training Center (FLETC) Criminal Investigator Training Program (CITP) on June 27, 2018. On October 5, 2018 I graduated from the Homeland Security Investigations Special Agent Training (HSISAT) training program. I have been involved in numerous investigations and enforcement actions involving the illegal smuggling of illicit substances. Prior to becoming a special agent, I was employed as a United States Border Patrol (USBP) Agent from August 2008 until May 2018. I have received formal and on-the-job training in the investigation of cases involving the sexual exploitation of children to include training programs, participation in the execution of search warrants involving child pornography, and participation in warrants involving seizures of computers and other digital storage media. I have conducted arrests and investigations of criminal alien smuggling cases as well as illicit substances smuggling cases since August of 2008. Prior to entering law enforcement, I was a firefighter and earned a degree in Fire Science from New Mexico State University.
2. The purpose of this application is to seize evidence, more particularly described in Attachment B, of violations of 18 U.S.C. §1470, which makes it a crime to use the mail or any facility or means of interstate or foreign commerce, to transfer obscene matter to another individual who has not attained the age of 16 years, knowing that such other individual has not attained the age of 16 years; 18 U.S.C. § 2251, which prohibits a person from employing, using, persuading, inducing, enticing and coercing a minor to engage in sexually explicit conduct for the purpose of producing

a visual depiction of such conduct; and 18 U.S.C. §§ 2252 and 2252A, which prohibit a person from producing, knowingly transporting, receiving, distributing, possessing or accessing with intent to view, in interstate or foreign commerce, or by using any facility or means of interstate or foreign commerce, child pornography, as defined in 18 U.S.C. Section 2256(8).

3. Because this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§ 1470, 2251, 2252, and 2252A will be found within the Samsung Galaxy S8 cell phone with IMEI: 357725081884174 ("SUBJECT CELLPHONE") utilized by Joseph Warren MONTGOMERY. (hereinafter "SUBJECT"), located in the evidence storage vault, HSI Douglas, Arizona.
4. To my knowledge, no prior attempt by investigative or legal process has been submitted to obtain the same or similar information sought in this warrant application. The target of the investigation is likely unaware of the existence of this investigation, has not been contacted, and therefore has made no statements to the effect that he would preserve the original data in lieu of seizure.
5. Based on my training and experience and the facts as set forth in this affidavit, there is Probable Cause to believe that violations of 18 U.S.C. 1470, 2251, 2252 and 2252A will be located on the SUBJECT CELLPHONE, further described in Attachment A. There is also Probable Cause to search the information described in Attachment A for evidence of these crimes, further described in Attachment B.
6. I am requesting that the court issue a search warrant directed to search the SUBJECT CELLPHONE, and to search the SUBJECT CELLPHONE to locate evidence of the production, possession, knowing access of, receipt and distribution of child pornography, enticement, and conclusively identify the user possessing and distributing child pornography, and associated with the aforementioned items to be searched.

7. To my knowledge, no prior attempt by investigative or legal process has been submitted to obtain the same or similar information sought in this warrant application.

**PERTINENT FEDERAL CRIMINAL STATUTES**

8. The purpose of this application is to seize evidence, more particularly described in Attachment B, of violations of 18 U.S.C. §1470, which makes it a crime to use the mail or any facility or means of interstate or foreign commerce, to transfer obscene matter to another individual who has not attained the age of 16 years, knowing that such other individual has not attained the age of 16 years; 18 U.S.C. § 2251, which prohibits a person from employing, using, persuading, inducing, enticing and coercing a minor to engage in sexually explicit conduct for the purpose of producing a visual depiction of such conduct; and 18 U.S.C. §§ 2252 and 2252A, which prohibit a person from producing, knowingly transporting, receiving, distributing, possessing or accessing with intent to view, in interstate or foreign commerce, or by using any facility or means of interstate or foreign commerce, child pornography, as defined in 18 U.S.C. Section 2256(8).

**DEFINITIONS**

9. The following non-exhaustive list of definitions applies to this Affidavit and Attachments A and B:
  - a. Child Pornography is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. See 18 U.S.C. 2256(8).
  - b. Child Erotica refers to materials or items that are sexually arousing to persons having a sexual interest in minors, but that are not, in and of themselves,

obscene or illegal. In contrast to "child pornography," this material does not necessarily depict minors in sexually explicit poses or positions. Some of the more common types of child erotica include photographs that are not sexually explicit, drawings, sketches, fantasy writing, and diaries. See Kenneth V. Lanning, *Child Molesters: A Behavioral Analysis* (2001) at 65. Federal courts have recognized the evidentiary value of child erotica and its admissibility in child pornography cases. See *United States v. Cross*, 928 F.2d 1030 (11th Cir. 1991) (testimony about persons deriving sexual satisfaction from and collecting non-sexual photographs of children admissible to show intent and explain actions of defendant); *United States v. Caldwell*, No. 97-5618, 1999 WL 238655 (E.D. Ky. Apr. 13, 1999) (child erotica admissible under Federal Rule of Evidence 404(b) to show knowledge or intent).

- c. Visual depictions include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. 2256(5).
- d. Minor refers to any person under the age of eighteen years. See 18 U.S.C. 2256(1).
- e. Sexually explicit conduct refers to actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. 2256(2).
- f. Cellular telephone: A cellular telephone (or mobile telephone, or wireless telephone) is a handheld wireless device used primarily for voice communication through radio signals. These telephones send signals through networks of transmitter/receivers called "cells," enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records

the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones now offer a broad range of capabilities. These capabilities include but are not limited to: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the devices.

- g. Digital device includes any electronic system or device capable of storing and/or processing data in digital form, including: central processing units; laptop or notebook computers; personal digital assistants; wireless communication devices such as telephone paging devices, beepers and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors and drives intended for removable media; related communications devices such as modems, cables and connections; storage media such as hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips; and security devices.
- h. Computer refers to an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. See 18 U.S.C. 1030(e)(1).
- i. Computer hardware consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed

disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices), peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

- j. Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic or other digital form. It commonly includes computer operating systems, applications and utilities.
- k. Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software or other related items.
- l. Computer passwords and data security devices consist of information or items designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to unlock particular data security devices. Data security hardware may include encryption devices, chips and circuit boards. Data security software of digital code may include programming code that creates test keys or hot keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide or booby-trap protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.
- m. Internet Service Providers or ISPs are commercial organizations, which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage and co-location of computers and other communications equipment. ISPs can offer various means by which to

access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or coaxial cable data transmission, dedicated circuits or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a coaxial cable system, and can access the Internet by using his or her account name and password.

- n. ISP Records are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files.
- o. Internet Protocol address or IP address refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a subscriber's computer at varying intervals at the discretion of the ISP. IP addresses might also be static meaning an ISP assigns a user's computer a specific IP address which is used each time the computer accesses the Internet.

- p. The terms records, documents and materials include all information recorded in any form, visual or aural, and by any means, whether in hand-made form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, printing and/or typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
- q. Digital device includes any electronic system or device capable of storing, processing, interpreting or rendering data in digital form, including computer systems of various form factors (computer desktop systems, towers, servers, laptops, notebooks and netbooks), personal digital assistants, cellular telephones and smart phones, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors and drives intended for removable media; related communication devices such as wired and wireless home routers and modems; storage media such as electro-mechanical hard disks, solid state hard disks, hybrid hard disks, floppy disks, optical disks such as compact disks and digital video disks, magnetic tapes and volatile and non-volatile solid state flash memory chips; and security devices including dongles and flash chips.
- r. Image or copy refers to an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. Imaging or copying maintains contents, but attributes may change during the reproduction.



- s. Hash value refers to a value generated after data has been subjected to a cryptographic mathematical algorithm. A hash value is akin to a digital fingerprint in that dissimilar data will not produce the same hash value after being subjected to the same hash algorithm. Therefore, a hash value is particular to the data from which the hash value was generated. Known hash values can be used to search for identical data stored on various digital devices and/or media as identical data will have the same hash value.
- t. Compressed file refers to a file that has been reduced in size through a compression algorithm to save disk space. The act of compressing a file will make it unreadable to most programs until the file is uncompressed.
- u. Remote storage refers to offsite data storage, where files are stored online, on a server or data storage device located elsewhere. Remote storage is typically accessible only with a user ID and password and can be accessed from any computer with Internet access. Often, remote storage locations can be mapped as a folder or drive on a computer where they can be accessed and used just like any other file, drive, or device connected to the computer. Typically this mapping is severed when a computer is logged off or powered off. Many remote storage service providers store data in an encrypted format, where the data can only be accessed with the user's user ID and password. In such cases, the service provider would not be able to access the data, or provide it to law enforcement, in an unencrypted form. If a remote storage location is attached or mapped to a computer, copying the data on-scene may be the only way to access the data in the future.

**BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY AND  
ONLINE CHILD EXPLOITATION**

10. I have been to training for the investigation of crimes involving the sexual exploitation of children. I am a computer user and have investigated crimes involving computers. Based on this training and knowledge, and the experience of other law enforcement personnel, I know the following:

11. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. Computer technology and the Internet revolutionized the way in which child pornography is produced, distributed, stored and communicated as a commodity and a further tool of child exploitation. For instance:

- a. Individuals can transfer photographs from a camera onto a computer-readable format with a variety of devices, including scanners, memory card readers, or directly from digital cameras, including those on most cellphones.
- b. Modems allow computers to connect to a network or another computer through the use of telephone, cable, or wireless connections. Electronic contact can be made to literally millions of computers around the world.
- c. The capability of a computer to store images in digital form makes the computer itself an ideal repository for child pornography. As explained further below, the storage capacity of electronic media used in home computers has increased tremendously within the last several years. These drives can store an extreme amount of visual images at very high resolution.
- d. The Internet, the World Wide Web and other Internet components afford individuals many different and relatively secure and anonymous venues for obtaining, viewing and trading child pornography or for communicating with others to do so or to entice children.
- e. Individuals can use online resources to retrieve, store and share child pornography, including services offered by Internet Portals such as Google, America Online (AOL), Yahoo! and Hotmail, among others. Online services allow a user to set up an account providing e-mail and instant messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. And even in cases where online

storage is used, evidence of child pornography can be found on the user's computer in most cases.

- f. As is the case with most digital technology, computer communications can be saved or stored on hardware and computer storage media used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite web sites in, for example, bookmarked files. However, digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or footprints in the web cache and history files of the browser used. Such information is often maintained for very long periods of time until overwritten by other data.
- g. The interaction between software applications and the computer operating systems often results in material obtained from the Internet being stored multiple times, and even in different locations, on a computer hard drive without the user's knowledge. Even if the computer user is sophisticated and understands this automatic storage of information on his computer's hard drive, attempts at deleting the material often fail because the material may be automatically stored multiple times and in multiple locations within the computer media. As a result, digital data that may have evidentiary value to this investigation could exist in the user's computer media despite, and long after, attempts at deleting it. A thorough search of this media could uncover evidence of receipt, distribution and possession of child pornography.
- h. Data that exists on a computer is particularly resilient to deletion. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years

at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensic tools. When a person deletes a file on a home computer, the data contained in the file does not actually disappear, rather, the data remains on the hard drive until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space, that is, in space on the hard drive that is not allocated to an active file and is left unused and free to store new data. Such residual data may remain in free space for long periods of time before it is overwritten by new data. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity and computer habits.

**BACKGROUND ON COMPUTERS AND EVIDENCE ASSESSMENT  
PROCESS IN CHILD PORNOGRAPHY AND CHILD EXPLOITATION  
INVESTIGATION**

12. This warrant seeks permission to locate not only computer files that might serve as direct evidence of the crimes described in the warrant, but also for evidence that establishes how and when computers were used to commit the specified crimes, and who used them.
13. As described above and in Attachment B, this application seeks permission to search and seize certain records that might be found in the SUBJECT CELLPHONE, in whatever form they are found. One form in which the records might be found is stored on a hard drive, or other electronic media. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some

of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis. In addition to user-generated documents (such as word processor, picture and movie files), Cell phones can contain other forms of electronic evidence that are not user-generated. In particular, a cell phone may contain records of how and when a cell phone was used, the purposes for which it was used, and who has used the records, as described further in the attachments.

14. Based upon my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that segregating information before commencement of the review of digital evidence by the examining agent is inconsistent with the evidence assessment process in child pornography and online child exploitation investigations. This is true in part because the items to be searched may not only contain child pornography but may also identify the user/possessor of the child pornography as well as the programs and software used to obtain the child pornography, which may be located on the cell phone to be searched. In addition, it is not possible to know in advance which storage media will contain evidence of the specified crimes, and often, such evidence is contained on more than one digital storage device. Further:

- a. Searching digital devices can be a highly technical process that requires specific expertise, specialized equipment and knowledge of how electronic and digital devices are often used in child pornography and online child exploitation matters. There are so many types of digital devices and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search.
- b. Because of the numerous types of digital devices and software that may contain evidence in child pornography and online child exploitation cases, it may also be necessary to consult with specially trained personnel who have specific expertise in the type of digital device, software application or operating system that is being searched in an off-site and controlled

- laboratory environment.
- c. Because digital data is particularly vulnerable to inadvertent or intentional modification or destruction, searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed, encrypted or password-protected data. Data hiding analysis can be useful in detecting and recovering such data and may indicate knowledge, ownership, or intent. The recovery of “hidden” data is highly specialized and time-intensive. For this reason, on-site key word searches are not sufficient to recover inadvertently or intentionally modified or destroyed data. Similarly, running hash values on-site to find files that contain child pornography is not an adequate on-site review and seizure procedure, because while hash values locate previously identified files of child pornography, they do not capture files that are the result of new production, images imbedded in an alternative file format, or images altered, for instance, by a single pixel. As a result, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of data stored on digital devices.
  - d. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or approximately 1,000 megabytes, is the equivalent of approximately 500,000 double-spaced pages of text. Storage devices capable of storing 500 gigabytes (GB) of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 240 million pages of data. Further, a 500 GB drive could contain as many as approximately 450 full run movies or 450,000 songs. As examining this quantity of data can take weeks or months, depending on the volume of the data stored, it would be

impractical to attempt this kind of data search on-site.

- e. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a cell phone, deleted or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a cell phone, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment.
- f. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users may also attempt to conceal data by using encryption, which means that a password or physical device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed

when the image file is opened. "Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed." A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

- g. Further, in finding evidence of how a digital device has been used, the purposes for which it was used, and who has used it, sometimes it is necessary to establish that a particular thing is not present on a hard drive or that a particular person (in the case of a multi-user cell phone) was not a user of the digital device during the time(s) of the criminal activity. For instance, based upon my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that when a digital device has more than one user, files can contain information indicating the dates and times that files were created as well as the sequence in which they were created, so that evidence of whether a user accessed other information close in time to the file creation dates, times and sequences can help establish user identity and exclude other users from using a digital device during relevant times.
- h. Because the absence of particular data on a digital device may provide evidence of how and when a digital device has been used, what it has been used for, and who has used it, analysis of the digital device as a whole may be required to demonstrate the absence of particular data. Such evidence of the absence of particular data on a digital device is not segregable from the digital device.
- i. The types of evidence described above may be direct evidence of a crime, indirect evidence of a crime indicating the location of evidence or a space where evidence was once located, contextual evidence identifying a digital device user, and contextual evidence excluding a digital device user. All of these types of evidence may indicate ownership, knowledge, and intent. This



type of evidence is not “data” that can be segregated, that is, this type of data cannot be abstractly reviewed and filtered by a seizing or imaging agent and then transmitted to investigators. Rather, evidence of this type is a conclusion, based on a review of all available facts and the application of knowledge about how a digital device behaves and how digital devices are used. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

- j. Based upon my knowledge, training and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that it is typically necessary to seize electronic devices capable of storing digital evidence as described in the Affidavit and Attachment B for off-site review because digital device searches involve highly technical, complex, time-consuming and dynamic processes.

#### **SEARCH METHODOLOGY TO BE EMPLOYED**

15. As noted within this search warrant, it would be extremely difficult, if not impossible to conduct a thorough on-site review of all of the potential evidence in this case. Given these constraints, the search methodology to be employed as to computers and digital media is as follows:

- a. Consistent with the information provided within this affidavit, contextual information necessary to understand the evidence, to identify the user/possessor of the child pornography, and to establish admissibility of the evidence in subsequent legal proceedings will also be sought by investigative agents.
- b. Additional techniques to be employed in analyzing the seized item will include (1) surveying various file directories and the individual files they contain; (2) opening files to determine their contents; (3) scanning storage areas, (4) performing key word searches through all electronic storage areas

to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in this affidavit and its attachments, and (5) performing any other data analysis techniques that may be necessary to locate and retrieve the evidence described in this affidavit and its attachments.

- c. Because it is expected that the SUBJECT CELLPHONE may constitute (1) instrumentality of the offense, (2) fruit of criminal activity, (3) contraband, or (4) evidence otherwise unlawfully possessed, it is anticipated that such evidence will not be returned to the owner and that it will be either forfeited or ultimately destroyed in accordance with the law at the conclusion of the case. However, if after careful inspection investigators determine that the CELLPHONE does not contain (1) instrumentality of the offense, (2) fruit of criminal activity, (3) contraband, (4) evidence otherwise unlawfully possessed, or (5) evidence of the person who committed the offense and under what circumstances the offense was committed, then such items seized will be returned.

#### **DETAILS OF THE INVESTIGATION**

16. Homeland Security Investigations Douglas, AZ ("HSI Douglas"), Child Exploitation Group ("CEG") Special Agents ("SA") have been monitoring various websites to identify individuals sexually exploiting children. Website A<sup>1</sup> is a website designed for adults to find sexual partners but is known to law enforcement as having members actively sexually exploiting children as well. Specifically, in connection with this warrant, HSI Douglas agents, acting in an undercover (UC) capacity, identified and had contact with an individual who confirmed his willingness to sexually abuse a child.

---

<sup>1</sup> In the interest of protecting ongoing investigations involving the website, your Affiant will not list it here.

17. On or about February 14 through 15, 2019, HSI agents accessed Website A posing as a 14-year-old girl in the Sierra Vista, AZ area and were solicited by an account, "introverted extrovert" (herein "MONTGOMERY").
18. On February 14, 2019, MONTGOMERY initiated the chat with the UC agent and was informed he was speaking with a 14 year old girl. MONTGOMERY continued to chat with the UC until approximately 8:20 P.M. that night. On the morning of February 15, 2019 at approximately 10:37 A.M. MONTGOMERY resumed chatting with the UC.
19. During the course of the chat MONTGOMERY referred to the UC as "kitten and princess". MONTGOMERY brought up the subject of Daddy Dom/Little girl (ddl) and explained what it meant to the UC.
20. On the afternoon of February 15, 2019 MONTGOMERY began making sexually explicit comments and asked to meet the UC for the purposes of sexual contact. MONTGOMERY made plans with the UC to meet and to drive to "the river" to have sex.
21. MONTGOMERY asked the UC if they were law enforcement and asked for proof that the UC was not working for law enforcement.
22. MONTGOMERY arrived at the agreed upon location in Sierra Vista, Arizona on February 15, 2019, as planned. HSI Special Agents observed a grey SUV drive by the parking lot where the meeting was to take place. A few minutes after MONTGOMERY was seen driving by the meet location he stated to the UC "I just drove by there and didn't see you."
23. MONTGOMERY was taken into custody, and after waiving his Miranda rights, MONTGOMERY stated that he came to the meet location for the purpose of having sex with the underage minor. MONTGOMERY, who had condoms in his possession, admitted that he knew the girl he was meeting was under the age of 18 and stated that her age didn't matter to him when he was planning to meet her.
24. When he was arrested, MONTGOMERY had the SUBJECT CELLPHONE in his possession. The SUBJECT CELLPHONE is currently in the lawful possession of

Homeland Security Investigations (HSI) and stored at 2334 East Highway 80 Douglas, AZ 85635.

25. MONGTOMERY consented to a search of the SUBJECT CELLPHONE. While conducting a search of the SUBJECT DEVICE for evidence of the UC chat, your affiant discovered what appeared to be based on training and experience, evidence of child pornography.
26. The search of the SUBJECT DEVICE immediately ceased, and the SUBJECT CELLPHONE was returned to the evidence vault.
27. MONTGOMERY is currently indicted under 4:19-CR-00689-RM-LAB for violation of 18 U.S.C. § 2422, Coercion and Enticement.

#### **RETURN AND REVIEW PROCEDURES**

28. Pursuant to Rule 41 of the Federal Rules of Criminal Procedure, I understand and will act in accordance with the following:
  - a. Pursuant to Rule 41(e)(2)(A)(i), an agent is required to file with the court an inventory return, that is, an itemized list of the property seized, within fourteen (14) days of the execution of the warrant.
  - b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized or copied on-site after the issuance of the warrant, not the later review of the media or information seized, or the later off-site digital copying of that media.
  - c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be limited to a description of the physical storage media that was seized or copied, not an itemization of the information or data stored on the physical storage media. Under Rule 41(f)(1)(B), I may retain a copy of that information for purposes of the investigation. Where possible, the government intends to make and retain a full image copy of the seized media, so that a copy of the evidence, rather than the original evidence, can be examined. The government will seize and retain both the original evidence


and any copies of this evidence. This procedure will ensure that the original evidence remains intact and that potential child pornography and instrumentalities of such crime will not be returned to the subject.

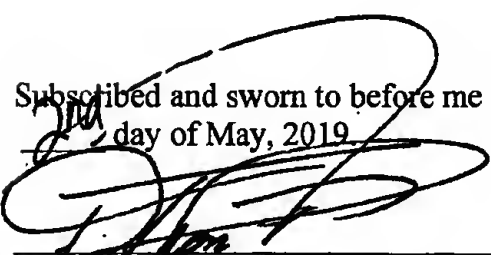
29. The warrant applied for would authorize the search of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e) (2) (B).

**CONCLUSION**

30. Based on the foregoing, I submit that this affidavit supports probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 1470, 2251, 2252, 2252A and 2422, are be located within the SUBJECT CELLPHONE. I therefore respectfully request that a search warrant issue authorizing a search of the SUBJECT CELLPHONE (described in Attachment A) for items set forth in Attachment B.

Respectfully submitted,

  
Daniel Sutcliffe  
Special Agent, HSI

  
Subscribed and sworn to before me this  
day of May, 2019.

D. Thomas Ferraro  
United States Magistrate Judge